PATENT ABSTRACTS OF JAPAN

(11)Publication number : **2000-269959**
(43)Date of publication of application : **29.09.2000**

(51)Int.Cl. **H04L 9/32**
H04Q 7/38
H04L 9/08

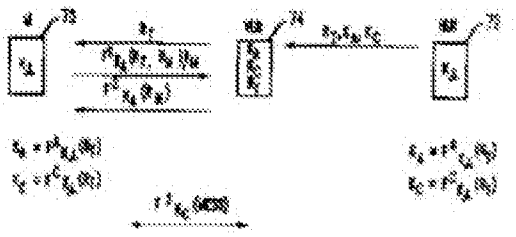
(21)Application number : **11-317628**
(22)Date of filing : **09.11.1999**

(71)Applicant : **LUCENT TECHNOL INC**
(72)Inventor : **BERENZWEIG ADAM L**
BRATHWAITE CARLOS ENRIQUE

(30)Priority
Priority number : **98 188818** Priority date : **09.11.1998** Priority country : **US**

(54) AUTHENTICATION METHOD BY UPDATED KEY

(57)Abstract:
PROBLEM TO BE SOLVED: To obtain an efficient authentication execution method that uses an authentication call sent to a terminal so as to supply information about the authentication, and to calculate an encryption key to the terminal.
SOLUTION: A visiting authentication center obtains a random number RT, an authentication key KA, and an encryption key KC from a host authentication center. The visiting authentication center transmits a random number RT to a transmitter to update an authentication key and an encryption key of the terminal and calls the terminal as a part of an authentication process. The terminal calculates the authentication key KA and the encryption key KC by using the RT and replies the call from the visiting authentication center. In addition, a reply of a visiting network to the authentication call of the terminal to the network is checked by using the authentication key.



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2000－269959
（P2000－269959A）
(43)公開日　平成12年９月29日(2000.9.29)

(51)Int.Cl.[7]	識別記号	ＦＩ		テーマコード（参考）
Ｈ０４Ｌ	9/32	Ｈ０４Ｌ	9/00	６７５Ｄ
Ｈ０４Ｑ	7/38	Ｈ０４Ｂ	7/26	１０９Ｒ
Ｈ０４Ｌ	9/08	Ｈ０４Ｌ	9/00	６０１Ｂ
				６７５Ｂ

審査請求　未請求　請求項の数20　ＯＬ　（全　７　頁）

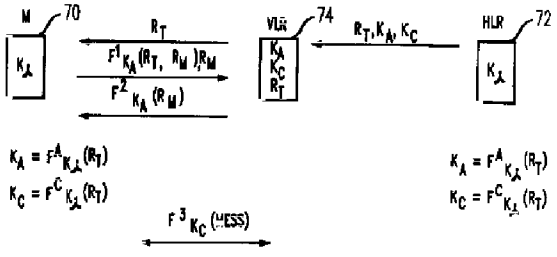
(21)出願番号　特願平11－317628
(22)出願日　平成11年11月９日(1999.11.9)
(31)優先権主張番号　０９／１８８８１８
(32)優先日　平成10年11月９日(1998.11.9)
(33)優先権主張国　米国（ＵＳ）

(71)出願人　596092698
ルーセント　テクノロジーズ　インコーポレーテッド
アメリカ合衆国．07974－0636　ニュージャーシィ，マレイ　ヒル，マウンテン　アヴェニュー　600
(72)発明者　アダム　エル．ブレンズウェイグ
アメリカ合衆国　10003　ニューヨーク，ニューヨーク，ナンバー12－０，イースト　ツエルヴス　ストリート　70
(74)代理人　100064447
弁理士　岡部　正夫　（外11名）

最終頁に続く

(54)【発明の名称】　キー更新による認証方法

(57)【要約】
【課題】　本発明は、端末装置に伝送された認証呼掛けを用い、認証と暗号キー値を計算するための情報を端末装置に供給する、効率的な認証実行方法を提供することを目的とする。
【解決手段】　ビジティング認証センタはホーム認証センタより、ランダム値ＲＴ、認証キー値ＫＡ、および暗号キー値ＫＣを得る。ビジティング認証センタはランダムナンバＲＴを端末装置に伝送し、端末装置の認証キーと暗号キー値とを更新し、また、認証プロセスの部分として端末装置に呼掛けする。端末装置はＲＴを用いて認証キー値ＫＡおよび暗号キー値ＫＣを計算し、かつ、ビジティング認証センタの呼掛けに応答する。加え、認証キー値を用いて、ネットワークへの端末装置の認証呼掛けに対するビジティングネットワークの応答を検査する。



【特許請求の範囲】
【請求項１】　認証方法において、
第一の値を端末装置に伝送するステップと、
第一の応答値が、入力として第一の値の少なくとも第一の部分およびキー入力として第一のキー値とを用いる第一の暗号関数の少なくとも出力の部分であり、第一のキー値が、入力として第一の値の少なくとも第二の部分およびキー入力として第二のキー値とを用いる第二の暗号関数の出力の少なくとも一部分であって、少なくとも第一の応答値を有する端末装置からの応答を受信するステップと、第一の応答値が予測された第一応の答値と等しいことを検査するステップとからなる認証方法。
【請求項２】　請求項１に記載の方法において、第二のキー値は端末装置と関連することを特徴とする方法。
【請求項３】　請求項１に記載の方法において、第一の暗号関数および第二の暗号関数は同一であることを特徴とする方法。
【請求項４】　請求項１に記載の方法において、第一の部分と第二の部分は同一であることを特徴とする方法。
【請求項５】　請求項１に記載の方法において、応答が第二の応答値を有し、第二の値を端末装置に伝送するステップをさらに有し、第二の値は入力として第二の応答値の少なくとも一部分とキー入力として第三のキー値とを用いる、第三の暗号関数の出力の少なくとも一部分であることを特徴とする方法。
【請求項６】　認証方法において、
第一の値を端末装置に伝送するステップと、
第一の応答値が、入力として第一の値の少なくとも第一の部分と第二の応答値の少なくとも第一の部分とキー入力として第一のキー値とを用いる第一の暗号関数の少なくとも出力の部分であり、第一のキー値が、入力として第一の値の少なくとも第二の部分およびキー入力として第二のキー値とを用いる第二の暗号関数の出力の少なくとも一部分であって、少なくとも第一の応答値と第二の応答値とを有する端末装置からの応答を受信するステップと、
第一の応答値が予測された第一の応答値と等しいことを検査するステップとからなる認証方法。
【請求項７】　請求項６に記載の方法において、第二のキー値は端末装置と関連することを特徴とする方法。
【請求項８】　請求項６に記載の方法において、第一の暗号関数および第二の暗号関数は同一であることを特徴とする方法。
【請求項９】　請求項６に記載の方法において、第一の値の第一の部分と第二の部分は同一であることを特徴とする方法。
【請求項１０】　請求項６に記載の方法において、第二の値を端末装置に伝送するステップを有し、第二の値は入力として第二の応答値の少なくとも第二の部分とキー入力として第三のキー値とを用いる第三の暗号関数の出力の少なくとも一部分であることを特徴とする方法。
【請求項１１】　認証方法において、
第一の値を受信するステップと、
第一の応答値が、入力として第一の値の少なくとも第一の部分とキー入力として第一のキー値とを用いる第一の暗号関数の少なくとも出力の部分であり、第一のキー値が、入力として第一の値の少なくとも第二の部分とキー入力として第二のキー値とを用いる第二の暗号関数の出力の少なくとも部分であって、少なくとも第一の応答値を有する応答を伝送するステップとからなる認証方法。
【請求項１２】　請求項１１に記載の方法において、第一の暗号関数および第二の暗号関数は同一であることを特徴とする方法。
【請求項１３】　請求項１１に記載の方法において、第一の部分と第二の部分は同一であることを特徴とする方法。
【請求項１４】　請求項１１に記載の方法において、応答は第二の応答値を有し、第二の値を受信するステップをさらに含み、第二の値は、入力として第二の応答値の少なくとも一部分とキー入力として第三のキー値とを用いる第三の暗号関数の出力の少なくとも一部分であることを特徴とする方法。
【請求項１５】　請求項１４に記載の方法において、第二の値が予測された第二の値と等しいことを検査するステップをさらに含む方法。
【請求項１６】　認証方法において、
第一の値を受信するステップと、
第一の応答値が、入力として第一の値の少なくとも第一の部分と第二の応答値の少なくとも第一の部分とキー入力として第一のキー値とを用いる第一の暗号関数の少なくとも出力の部分であり、第一のキー値が、入力として第一の値の少なくとも第二の部分とキー入力として第二のキー値とを用いる第二暗号関数の出力の少なくとも一部分であって、少なくとも第一の応答値と第二の応答値とを有する応答を伝送するステップとからなる認証方法。
【請求項１７】　請求項１６に記載の方法において、第一の暗号関数および第二の暗号関数は同一であることを特徴とする方法。
【請求項１８】　請求項１６に記載の方法において、第一の値の第一の部分と第二の部分は同一であることを特徴とする方法。
【請求項１９】　請求項１６に記載の方法において、第二の値を受信するステップをさらに含み、第二の値は、入力として第二の応答値の少なくとも一部分とキー入力として第三のキー値とを用いる第三の暗号関数の出力の少なくとも一部分であることを特徴とする方法。
【請求項２０】　請求項１９に記載の方法において、第二の値が予測された第二の値と等しいことを検査するステップを有することを特徴とする方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は通信に関するものであり、さらに詳しく言うと、無線通信システムにおける通信者の認証に関するものである。

【０００２】

【従来の技術】図１は、基地局１０と、これと関連するセル１２と、セル１２内にあるモバイル１４とを示している。最初に、モバイル１４が基地局１０との通信をレジスタするか、又は通信を試みる場合、モバイルの通信ネットワークへのアクセスが許可される前に、基地局１０がモバイル識別検査、認証を行う。モバイル１４がそのホームネットワーク以外のネットワーク内にある場合、ビジティングネットワーク内にあるとして認証が行われる。ホームネットワークとは、モバイル端末所有者と契約を交し、無線通信サービスを提供するサービスプロバイダによって制御がなされるネットワークのことをいう。モバイルがビジティング通信ネットワークで作動する場合、基地局１０がモバイルを認証する際、モバイルのホームネットワークの認証センタ１６との通信が必要となる。図１の例においては、モバイル１４はビジティングネットワーク内にある。結果、モバイル１４の認証にはモバイルのホームネットワークの認証センタ１６との通信を必要とする。モバイル１４がビジターネットワークにアクセスを試みると、基地局１０はビジティング通信ネットワークの認証センタ１８との通信を行う。認証センタ１８は、モバイル１４の電話番号といったようなモバイルや端末の識別子によって、モバイル１４がホーム認証センタ１６を使用するネットワークにレジスタされていることを判断する。次に、ビジティング認証センタ１８はＩＳ４１信号ネットワーク２０のようなネットワーク上でホーム認証センタ１６と通信を交す。次に、ホーム認証センタ１６は、モバイル１４の登録エントリを有するホーム位置レジスタ２２にアクセスする。ホーム位置レジスタ２２は、モバイルの電話番号といったような識別子によって端末もしくはモバイルと連動する。ホーム位置レジスタに蓄積された情報は、暗号キー発信や、ビジタ認証センタのビジター位置レジスタ２４に供給される他の情報の発信に使用される。次に、ビジター位置レジスタ２４からの情報は、モバイル１４に伝送される情報を基地局１０に供給することに使用される。これにより、モバイル１４は応答可能となり、かつ、それにより通信サービスを受ける資格を有したモバイルであるとの認証がなされる。

【０００３】図2は、ＧＳＭ無線ネットワークで使用される認証工程図である。この場合、モバイルとホーム位置レジスタの両方はキーＫｉを有する。モバイルがビジティングネットワークへのアクセスをリクエストすると、ビジティング認証センタはホーム認証センタにコンタクトし、変数ＲＡＮＤ、ＳＲＥＳ、およびＫｃを受取る。ホーム認証センタはモバイルと関連するホーム位置レジスタからの値Ｋｉを使用し、値ＳＲＥＳ、および値Ｋｃを発する。値ＳＲＥＳは、入力としてランダムナンバＲＡＮＤ、かつ、キー入力として値Ｋｉとにより、Ａ３として知られる暗号関数を用いて計算される。同様の方法で、暗号キーＫｃは、入力としてＲＡＮＤ、かつ、キー入力として値Ｋｉとにより、暗号関数Ａ８を用いて計算される。これらの値はビジティング認証センタのビジー位置レジスタに転送される。次に、ビジティング認証センタはモバイルにランダムナンバＲＡＮＤを伝送することにより、モバイルに呼掛けする。モバイルは、ホーム認証センタによって行われた計算方法と同方法でＳＲＥＳ、およびＫｃを計算する。次にモバイルは、値ＳＲＥＳをビジティング認証センタに伝送し、そこでビジティング認証センタはモバイルより受信のＳＲＥＳとホーム認証センタから受信のＳＲＥＳとを比較する。これらの値がマッチした場合、モバイルのビジティングネットワークへのアクセスが許可となる。モバイルと、ビジティングネットワーク間の通信がさらに暗号化される場合、入力として暗号化されるメッセージと、かつ、値Ｋｃと等しいキー入力とにより、Ａ５暗号関数を用いることにより、これらが暗号化される。暗号関数Ａ３、Ａ５、およびＡ８は従来技術でよく知られており、ＧＳＭ標準により推奨されている。ＧＳＭシステムにおいて、ホーム認証センタとの通信を含むこの認証プロセスは、モバイルがビジティングネットワークで新規コールを開始する毎に実行される。

【０００４】図３ａおよび図３ｂは、ＩＳ４１コンプライアントネットワークに使用される認証プロセス図である。ＩＳ４１コンプライアントネットワーク例は、ＡＭＰＳ（アドバンスドモバイルホンサービス）、ＴＤＭＡ（時分割多元接続）、もしくはＣＤＭＡ（コード分割多元接続）プロトコルを用いるネットワークである。このシステムにおいて、モバイルとホーム位置レジスタの両方はＡＫＥＹと呼ばれるシークレット値を含んでいる。モバイルがビジティングネットワークへのアクセスをリクエストすると、ビジティングネットワーク認証センタはホーム認証センタからのデータをリクエストする。実際の認証プロセス開始前に、モバイルとビジター位置レジスタとの両方に認証および通信のための暗号アルゴリズムにて使用されるキーを供給することによりキー更新が実行される。モバイルと関連するホーム位置レジスタは、モバイルの電話番号といったような識別子を用い所在場所が確認され、また、ホーム位置レジスタに保存されたＡＫＥＹ値は、ビジター位置レジスタへの伝送データを作り出すことに使われる。計算された値は、ＳＳＤＡ（共用シークレットデータＡ）値とＳＳＤＢ（共用シークレットデータＢ）値である。これらの値は、入力としてランダムナンバＲｓと、キー入力として値ＡＫＥＹとを用い、ＣＡＶＥアルゴリズムを実行することにより

計算される。ＣＡＶＥアルゴリズムは、従来技術でよく知られており、ＩＳ４１スタンダードに詳述されている。ホーム認証センタは値Ｒｓ、ＳＳＤＡ、およびＳＳＤＢを、ビジティングネットワークのビジター位置レジスタに転送する。これをうけて、ビジティングネットワークは、Ｒｓをモバイルに伝送することにより、モバイルで使用されることになる共用シークレットデータ（ＳＳＤＡおよびＳＳＤＢ）を更新する。次に、モバイルは、ホーム認証センタにより行われた方法と同計算方法でＳＳＤＡおよびＳＳＤＢを計算する。ここでモバイルとビジター位置レジスタの両方がＳＳＤＡ値およびＳＳＤＢ値を有することで認証プロセスが開始される。

【０００５】図３ｂは、モバイルとビジター位置レジスタとの両方がキーＳＳＤＡおよびＳＳＤＢを受取った後、いかにモバイルがビジティングネットワーク内で認証されるかを示したものである。ビジティング認証センタは、ランダムナンバＲＮをモバイルに送信することによりモバイルに呼掛けを行う。この時点で、モバイルとビジティング認証センタの両方は値ＡＵＴＨＲを計算する。ＡＵＴＨＲは、入力としてランダムナンバＲＮと、キー入力としてＳＳＤＡ値とを用いるＣＡＶＥアルゴリズムの出力と等しい。次にモバイルは計算された値ＡＵＴＨＥＲをビジティング認証センタに伝送する。ビジティング認証センタはそのＡＵＴＨＥＲの計算値と、モバイルから受信した値との比較を行う。値がマッチした場合、モバイルは認証され、ビジティングネットワークへのアクセスが可能となる。加え、モバイルとビジティング認証センタの両方は、暗号キーＫｃの値を計算する。値Ｋｃは、入力として値ＲＮと、キー入力として値ＳＳＤＢとを用いるＣＡＶＥアルゴリズムの出力と等しい。この時点で、モバイルとビジティングネットワーク間の通信が許可され、暗号関数を用いて暗号化されるであろう。そこで、入力は暗号化されるメッセージと、キーＫｃである。暗号関数はそれぞれの標準によってＣＤＭＡシステムおよびＴＤＭＡシステムが指定される。ＩＳ４１に関して、ビジティング認証センタとホーム認証センタ間の通信は、モバイルに呼出しされる度毎ではなく、モバイルがビジティングネットワークにレジスタする度毎にのみ行われることを注記する。

【０００６】上述の方法は、モバイルがネットワークにアクセスする許可を得るためのその検査方法を示したものである。しかし、上記の方法では正規ネットワークによりそれ自身を確認することが問われるモバイル検査については論じていない。図４は、ビジティングネットワークとモバイル間の相互認証を可能にするＩＳ４１スタンダードの改善案である。図４は、図３ａに関して上記で論じたように、一旦、モバイルとビジター位置レジスタの両方が値ＳＳＤＡおよび値ＳＳＤＢを受取った時の相互認証プロセスを図示したものである。ビジティングネットワークはランダムナンバＲＮを伝送することによりモバイルに呼掛けを行う。次に、モバイルは計算実行により応答し、入力として値ＲＮおよびＲＭと、キー入力として値ＳＳＤＡとを用い、暗号関数Ｆ１の出力を得る。この場合、ＲＮはビジティングネットワークにより伝送された値と同値であり、ＲＭはモバイルにより計算が行われたランダムナンバである。暗号関数の出力伝送に加え、値ＲＭもまた非暗号化フォームでビジティングネットワークに伝送される。ビジティングネットワークは、キー入力として値ＳＳＤＡにより、Ｆ１暗号関数への入力としてＲＭの非暗号化フォームと値ＲＮとを用いて、Ｆ１暗号関数の出力を計算する。この出力値は、モバイルから受取った値と比較され、これらがマッチした場合、モバイルが検査、認証される。次に、ビジティングネットワークは、値ＲＭのフォームでモバイルより供給された呼掛けに応答することによって、モバイルにより認証、検査される。ビジティング認証センタは、入力として値ＲＭと、キー入力として値ＳＳＤＡとを用いて、暗号関数Ｆ２の出力を伝送する。次に、モバイルは同様の計算を行い、キー値ＳＳＤＡおよび値ＲＭとを用いて、ビジティングネットワークから受取った値と、暗号関数Ｆ２の出力から得た値とを比較する。これらの値がマッチした場合、モバイルは認証、検査されたネットワークを考え、そのネットワークとの通信を継続する。ビジティング認証センタとモバイルの両方は、入力として値ＲＮおよびＲＭと、キー入力として値ＳＳＤＢとを用いて、暗号関数Ｆ３の出力を得ることにより、暗号キーＫＣの値を計算する。この時点で、モバイルとビジティングネットワークとが通信可能となる。この時、万一、暗号通信が所望される場合、入力として暗号化されるメッセージと、キー入力として値ＫＣとにより、暗号アルゴリズムＦ４を用い、メッセージが暗号化される。暗号関数Ｆ１、Ｆ２、およびＦ３は、ハッシュ関数であるか、又はＳＨＡ－１等の１つの暗号関数であり、関数Ｆ４はＤＥＳであるような暗号関数であろう。ハッシュ関数や、ＳＨＡ－１といったような一方向性暗号関数や、ＤＥＳといったような暗号関数は従来技術においてよく知られている。

【０００７】

【発明が解決しようとする課題】しかしながら、上述の従来の相互認証プロセスにおいては、認証プロセスが開始する前に、モバイルとビジター位置レジスタとの両方が値ＳＳＤＡおよび値ＳＳＤＢとを有することが必要であることから、その非効率さに悩まされている。結果、モバイルとビジティング認証センタ間に少なくとも２セットの通信が必要となる。通信の第一セットにおいては、値ＳＳＤＡおよび値ＳＳＤＢの計算に使用される情報をモバイルに供給する。通信の第二セットでは、相互認証の実行に使用される。

【０００８】

【課題を解決するための手段】本発明は、認証及び暗号

翻訳キーの値を計算するために端末装置に情報を提供するように、端末装置に伝送される認証呼かけを使用することによって、認証を実行するためのより効果的な方法を提供する。結果、端末装置にキー値を供給するための別々の通信を必要とせず、非効率的な２セット通信を解消する。ビジティング認証センタはホーム認証センタより、ランダム値ＲＴ、認証キー値ＫＡ、および暗号キー値ＫＣを得る。ビジティング認証センタはランダムナンバＲＴを端末装置に伝送し、端末装置の認証キーと暗号キー値とを更新し、また、認証プロセスの部分として端末装置に呼掛けする。端末装置はＲＴを用いて認証キー値ＫＡおよび暗号キー値ＫＣを計算し、かつ、ビジティング認証センタの呼掛けに応答する。加え、認証キー値を用いて、ネットワークへの端末装置の認証呼掛けに対するビジティングネットワークの応答を検査する。

【０００９】

【発明の実施の形態】図５は、モバイルもしくは固定端末に伝送されたシングルランダム値を用いて、端末装置の認証および暗号キー値を更新し、さらに、端末装置への認証呼掛けを行う方法を図示したものである。モバイルもしくは固定端末７０、およびホーム位置レジスタ７２はキー値Ｋｉを共用する。モバイル端末７０がビジティングネットワークへのアクセスリクエストを行うと、ビジティング認証センタはホーム認証センタにコンタクトし、ランダム値ＲＴ、認証キー値ＫＡ、および暗号キー値ＫＣとを得る。このリクエストに応え、ホーム認証センタは、ビジティング認証センタ経由でモバイル端末より提供された電話番号等の識別子を用い、モバイル端末７０と関連するホーム位置レジスタ７２にアクセスする。次に、ホーム認証センタは、入力としてランダムナンバＲＴと、キー入力として値Ｋｉとを用いて、暗号関数ＦＡの出力を得ることにより認証キー値ＫＡを計算する。加え、ホーム認証センタは、入力として値ＲＴを、またキー入力として値Ｋｉとを用い、暗号関数ＦＣの出力を用いて暗号キー値ＫＣを計算する。一旦、これらの計算が行われると、ホーム認証センタは値ＲＴ、ＫＡ、およびＫＣをビジティング認証センタに通信する。ビジティング認証センタは、モバイル端末７０と関連するビジター位置レジスタに値ＫＡ、ＫＣおよびＲＴを保存する。次に、認証呼掛けとして、かつ、モバイル端末で使用された暗号キー値および認証を更新するために使用する値として、ビジティング認証センタは値ＲＴをモバイル端末７０に通信する。モバイル端末はビジティング認証センタより受取った値ＲＴを用い、ホーム認証センタで行った計算方法と同様の方法で、認証キー値ＫＡおよび暗号キー値ＫＣとを計算する。次に、モバイル端末は認証キー値ＫＡを用い、ビジティング認証センタの認証呼掛けに応答する。モバイル端末は入力として値ＲＴおよびＲＭと、かつ、キー入力として認証キー値ＫＡとを用いて、暗号関数Ｆ１の出力を判断する。しかし、入力として、ＲＴおよびＲＭの両方でなく、値ＲＴを用いることも可能である。暗号関数Ｆ１および値ＲＭの出力はビジティング認証センタに通信される。しかし、ＲＭが暗号関数Ｆ１の入力として使用されなかった場合や、ネットワークの認証が必要とされない場合は、値ＲＭの伝送は行われない。値ＲＭはモバイル端末により選択されたランダム値である。ビジティング認証センタは入力ＲＴおよびＲＭ、およびキー入力値ＫＡ により関数Ｆ１の出力値を計算する。それにより、モバイル端末より通信された値とその結果とが比較可能となる。値がマッチした場合、モバイル端末はビジティングネットワークにより、照合又は認証される。モバイル端末により供給された値ＲＭ は、モバイル７０によるビジティングネットワークへの認証呼掛けに用いられる。ビジティングネットワークは、入力として値ＲＭを、また、キー入力として値ＫＡとを用い関数Ｆ２の出力を計算する。この出力値はモバイル端末に通信される。モバイル端末は、入力として値ＲＭを、かつ、キー入力として値ＫＡとにより関数Ｆ２の出力を別個に判断し、これらの出力値がマッチした場合に、モバイル端末はビジティングネットワークの照合又は認証する。モバイル端末とビジティングネットワークの両方が互いに識別検査、認証を一旦行うと、通信は継続する。通信は非暗号化メッセージもしくは暗号化メッセージを用いることにより交わされる。暗号化メッセージが使用される場合、入力としてメッセージを、かつ、キー入力として暗号値ＫＣとにより、暗号関数Ｆ２の出力を用いてメッセージが暗号化される。このプロセスは、モバイル端末とビジティングネットワーク間においてコールが試みられる度毎に実行される。もしくは、コールが試みられるその度毎ではなく、モバイルがビジティングネットワークにレジスタする度毎にホーム認証センタにコンタクトすることも可能である。また、モバイルがビジティングネットワークにレジスタされたままであるかぎり、ＫＡ、ＫＣ、およびＲＴの同一値を使用することも可能である。暗号関数Ｆ１、Ｆ２、ＦＡ、およびＦＣはハッシュ関数であるか、もしくはＳＨＡ－１のような１暗号関数であろう。また、関数Ｆ３はＤＥＳのような暗号関数であろう。ハッシュ関数、ＳＨＡ－１のような一方向性暗号関数、およびＤＥＳのような暗号関数は従来技術によってよく知られている。

【００１０】モバイル端末がホームネットワーク内にある場合にも、同工程の実行が可能である。この場合、ビジティング認証センタではなく、ホーム認証センタがモバイル端末と通信を行う。無線通信において、端末と認証センタ間の通信は無線基地局を通過して行われる。

【図面の簡単な説明】

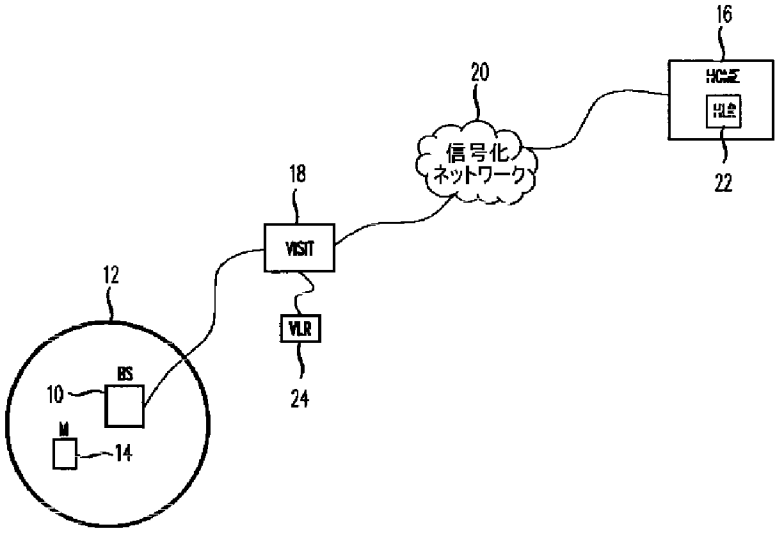
【図１】モバイル、ビジティングネットワーク、およびホームネットワーク間の通信を図示したものである。

【図２】ＧＳＭネットワークの認証プロセス図である。

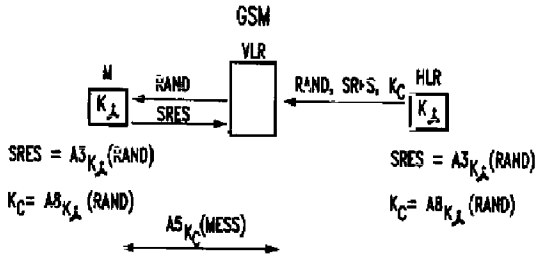
【図３ａ】ＩＳ４１コンプライアントネットワークのキ

ー更新および認証プロセスを図示したものである。
【図３ｂ】ＩＳ４１コンプライアントネットワークのキー更新および認証プロセスを図示したものである。
【図４】従来技術による相互認証方法を図示したもので
ある。
【図５】本発明によるキー更新および相互認証の実行方法である。

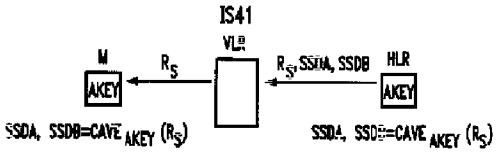
【図１】



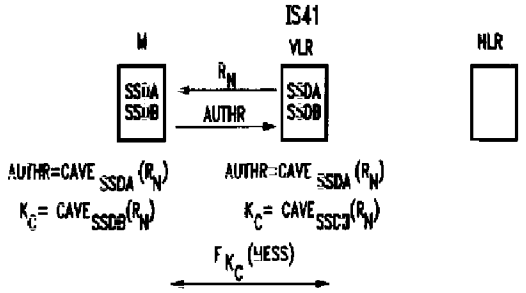
【図２】



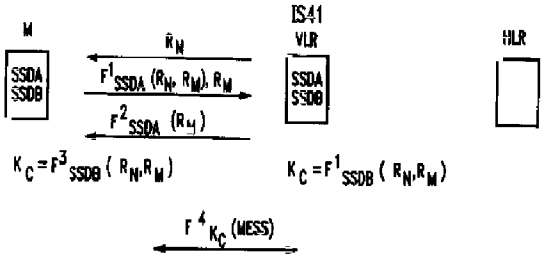
【図３ａ】



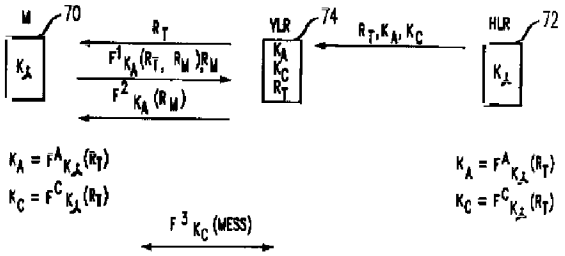
【図３ｂ】



【図４】



【図５】



フロントページの続き

(72)発明者　カルロス　エンリキュー　ブラスウェイト
アメリカ合衆国　07050　ニュージャーシィ，オレンジ，ヒルヤー　ストリート　63